INTERIM OPERATIONAL SYSTEMS DOCTRINE FOR THE REMOTE ACCESS SECURITY PROGRAM (RASP) SECRET DIAL-IN SOLUTION

SECTION I – INTRODUCTION

1. This doctrine contains the minimum security standards for the protection, handling, use, and control of the Remote Access Security Program (RASP) Secret Dial-In Solution. It also provides new doctrine for the use of RASP in fixed sites, and mandates that the FORTEZZA® Card (for Media Encryption) and FORTEZZA®-enabled Modem card be programmed under the RASP infrastructure using new RASP universals.

2. For the first universal changeover, the user must request and use a new certificate with new universals by 1 January 2002. For the second universal changeover, which commences on 1 October 2003, the user must request and use a new certificate with new universals by 31 December 2003. The use of the first universals must cease by 31 December 2003. The combination of both universal changeovers will permit extending the use of the RASP classified cards until 31 December 2005.

3. It is important for all present and prospective RASP users and implementers to receive this doctrine. Please note that the doctrine and procedures outlined herein for traveling users also applies to fixed site users, with differences specifically stated for environments formally approved for the protection of United States (U.S.) classified information (secure enclave) and facilities not approved for the protection of U.S. classified information (non-secure enclave).

4. This doctrine will remain in force until a formal instruction is issued through the National Security Telecommunications and Information Systems Security Committee (NSTISSC) incorporating this information.

SECTION II – CONFIGURATIONS

5. The RASP Solution can be configured in three ways: *RASP Secure Access™ (for mobile users), Enterprise RASP™ (for networks supporting large numbers of mobile users)*, or *Workplace RASP™* (for fixed-site users). The difference between the three configurations is described below. With all configurations, the user must use the appropriate FORTEZZA®-enabled modem to securely dial over a Public Switched Telephone Network (PSTN) to gain access to a protected enclave.

SECTION III - RASP SECRET DIAL-IN SOLUTION

6. A typical system implementing the ***RASP Secure Access*** solution is comprised of:

a. A PALLADIUM Secure Modem (a FORTEZZA®-enabled PCMCIA Modem) with X.509 FORTEZZA public key certificates for the protection of SECRET information;

b. The OPtiva Secure Plus™ Remote Access Server at the protected enclave boundary;

c. The optional RASP Secure Media for Windows NT4.0;

d. The optional FORTEZZA® Card with X.509 FORTEZZA® public key certificates for the protection of SECRET information, using the RASP Secure Media;

e. The computer that implements RASP.

7. A typical system implementing the ***Enterprise RASP*** solution is comprised of:

a. A RASP Secure Modem™ (a FORTEZZA-enabled PCMCIA Modem) with X.509 FORTEZZA® public key certificates for the protection of SECRET information;

b. The RASP Secure Access Server at the protected enclave boundary;

c. The RASP Authentication Server™ and RASP Audit Log™ for access control and audit logging;

d. The optional RASP Secure Media for Windows NT4.0;

e. The optional FORTEZZA® Card with X.509 FORTEZZA® public key certificates for the protection of SECRET information, using the RASP Secure Media;

f. The computer that implements RASP.

8. A typical system implementing the ***Workplace RASP*** solution is comprised of:

a. Either a *RASP Secure Access* configuration, or an *Enterprise RASP* configuration, PLUS

b. A Virtual Private Network (VPN) approved for RASP with RSA public key certificates for the protection of SECRET information. For specific configurations, refer to the RASP SIPRNET website at http://www.nsa.smil.mil/di/solutions/html/RASP.html.

SECTION IV – REQUIREMENTS

9. *Workplace RASP* users must acquire public key certificates for both the client and server component of the VPN from the SIPRNET, Intelink Management Office (IMO).

10. The RASP solution may only be used until 31 December 2005.

11. Traveling RASP users are encouraged to use the *Workplace RASP* solution to gain the additional communication channel security benefits afforded by the VPN. However, this is not required.

12. RASP users are required to read and sign a RASP User Agreement separate from this document.

13. System Administrators (SA) and Information System Security Officers (ISSO) are required to read and sign a RASP SA/ISSO Agreement, separate from this document.

14. SA's are required to follow specific architectural requirements/VPN configuration guidelines provided by the RASP Program Office. For Architecture Requirements, VPN configuration guidelines, and User/SA Agreement statements, contact NSA at 1-800-688-6115 or via SIPRNET at http://www.nsa.smil.mil/di/solutions/html/RASP.html.

15. RASP users are encouraged to use the RASP Secure Media to protect their data in the event their computer is lost or stolen.

SECTION V – COMMUNICATIONS CONNECTIVITY

16. The RASP solution shall only be used to connect to a SECRET network.

17. The user must use either the PALLADIUM Secure Modem to communicate through the OPtiva Secure Plus Remote Access Server or the RASP Secure Modem to communicate through the RASP Secure Access Server, to access the classified enclave.

18. To reduce the potential for exploitation of RASP Secret dial-in communications, a continuous connection to a network is not allowed. As a minimum, each single network connection made by a fixed site must not last more than twenty-four (24) hours. Traveling users who do not use the *Workplace RASP* solution are limited to a maximum total of four (4) hours connectivity in any single 24-hour period.

19. Access through unclassified, non-secure networks such as commercial Internet Service Providers (ISPs) is not permitted. All RASP users are prohibited from intentionally using the computer that implements RASP for communicating to a non-RASP solution.

SECTION VI – RESTRICTIONS

20. RASP users and SA's must be U.S. Government employees or contractors acting at the direction of the U.S. Government.

21. RASP users must be approved in writing by the appropriate department or agency to process classified (up to SECRET) information outside a
formally approved facility.

22. The PALLADIUM Secure Modem, RASP Secure Modem, and the optional FORTEZZA® Card for Media Encryption shall be programmed by a FORTEZZA® Certification Authority Workstation (CAW) capable of providing certificates from the Secret Certificate Management Infrastructure.

23. The Rivest Shamir Adleman (RSA) Certificate(s) for the *Workplace RASP* solution must be programmed by the IMO Certificate Authority.

24. The computer that implements RASP is considered sensitive and must be physically protected by: (a) either being in the user's continuous personal possession or (b) with an equivalently cleared responsible designee or (c) stored in a secure facility. If the chain of continuous control is broken, the user must consider the laptop, the FORTEZZA® card, and the FORTEZZA®-enabled PCMCIA modem exposed to potential exploitation. The user must not attempt to use the RASP solution and must contact the SA immediately. The SA must follow the procedures as outlined in the classified SA/ISSO Agreement. (In summary, A: If the laptop with no FORTEZZA® card or FORTEZZA®-enabled modem is lost or stolen, no COMSEC reportable action is required since all classified data has been encrypted; however, the user should contact the SA upon recovery of the laptop, and the SA must contact the ISSO for guidance. B: If the laptop, FORTEZZA® card and FORTEZZA®-enabled modem are lost or stolen, the user must contact the SA and the SA must contact the Certification Authorities (CA) that programmed the FORTEZZA® card and FORTEZZA®-enabled modem to revoke the user's certificates. Upon recovery of the equipment, the user must contact the SA and the SA must contact the ISSO for guidance.)

25. If the RASP Secure Media application is not implemented on the user's computer, the computer must be protected to the highest classification processed on it (normally SECRET). If the machine is lost or stolen, the user must follow local procedures for reporting the loss or theft of classified information.

SECTION VII – PHYSICAL SECURITY

26. Physical security is of paramount concern in the user environment. Users must be aware of their surroundings at all times when

processing SECRET information outside of a protected enclave. Users shall obtain a security threat briefing geared to their specific remote environments prior to the use of the RASP solution.

a. All RASP solution users must keep the FORTEZZA® card and FORTEZZA®-enabled Modem on their person or stored in a manner that will minimize the possibility of loss, theft, unauthorized use or tampering.

b. All RASP solution users should memorize their passphrases (PIN) for the FORTEZZA®-enabled Modem, the FORTEZZA® card, the VPN, and the BIOS boot password for the computer that implements RASP. If not memorized, the user must keep these passphrases separate from the corresponding devices. The FORTEZZA® card and the FORTEZZA®-enabled Modem must be kept separate from the computer that implements RASP when not in use, and must not be stored or carried in the same container as the computer that implements RASP.

SECTION VIII – CLASSIFICATION

27. The FORTEZZA® card, FORTEZZA®-enabled Modem, and computer that implements RASP are classified to the highest classification asserted by the certificates on that card. The level of data processed is normally SECRET whenever the Personal Identification Number (PIN) is inserted into the FORTEZZA® card and the card is unlocked.

28. The FORTEZZA®-enabled Modem card is classified to the highest classification asserted by the certificates on that card. The level of data processed is normally SECRET whenever the Personal Identification Number (PIN) is inserted into the FORTEZZA® card and the card is unlocked.

29. If RASP Secure Media is used, **all** information files, classified and unclassified (e.g. electronic message files, document files, graphic or image files), stored on the hard drive that implements RASP used for mobile/traveler/non-secure environment operations, must be encrypted by the FORTEZZA® card using the RASP Secure Media.

30. The hard drive protected by the RASP Secure Media is not classified while the information is fully encrypted (i.e. the PIN is not entered into the FORTEZZA® card and the card is not unlocked).

31. If the RASP Secure Media is not installed on the user's computer that implements RASP, the computer must be physically protected commensurate with the highest classification of information processed by the

computer that implements RASP (normally SECRET).

32. The computer that implements RASP must be physically handled, controlled, protected, and stored in a manner commensurate with the highest classification of data processed on the computer whenever the computer is on or is accessing/connected to the protected enclave.

SECTION IX – TAMPERING, LOSS, OR THEFT

33. RASP users must handle the RASP solution as specified in the User Agreement as well as regularly inspect their solution components for obvious signs of tampering (e.g. scratches, pry marks, scratched screws, loose connections, etc.). If the chain of continuous control is broken or there are signs of tampering, the user must consider the computer that implements RASP, the FORTEZZA® card, and the FORTEZZA®-enabled Modem exposed to potential exploitation.

34. If a RASP Secure Media enabled computer with no FORTEZZA® card or FORTEZZA®-enabled Modem is lost or stolen, no Communications Security (COMSEC) reportable action is required since all classified data has been encrypted. However, the user must contact/notify the SA of the loss/theft. Upon recovery of the computer that implements RASP, the user must notify the SA and the SA must contact the ISSO for guidance/approval before the computer that implements RASP may be used. If the RASP Secure Media application is not implemented on the user's computer, the computer must be protected to the highest classification processed on it (normally SECRET).

35. If the FORTEZZA® card or FORTEZZA®-enabled Modem are lost or stolen, the user must contact the SA, and the SA must contact the Organizational Registration Authority (ORA). The ORA must contact the CA who programmed the FORTEZZA® card or FORTEZZA®-enabled Modem so that an evaluation can be performed to determine the appropriate compromise or revocation action (placement of the user's certificate on the Certificate Revocation List (CRL), Compromised Key List (CKL) or Indirect Certificate Revocation List (ICRL)). The SA must also remove the compromised certificates from all Access Control Lists (ACL). Upon recovery of the equipment, the user must contact the SA and the SA must contact the Information System Security Officer (ISSO) for guidance before any equipment may be used.

36. If the SAs FORTEZZA® card, which was used to implement the Secure Media, is lost or stolen, the SA must report the loss to the ORA.

The ORA must contact the CA who programmed the FORTEZZA® card so that an evaluation can be performed to determine the appropriate compromise or revocation action (placement of the user's certificate on the CRL, CKL, or ICRL. All user computers that implement RASP serviced by that SA's FORTEZZA® card must be afforded extra protection until such time as the users computer's ACL has been updated to remove the lost personality or certificate within the affected domain(s) and the SA or local ISSO can determine that the computer that implements RASP has not been tampered with or otherwise compromised.

SECTION X – SHARED CERTIFICATES

37. The FORTEZZA®-enabled modems are a relatively high-cost item, and may be loaded with shared certificates to facilitate sharing (more than one individual using a computer that implements RASP). The SA must maintain some form of tracking to identify who has the FORTEZZA®-enabled Modem card at any given time.

SECTION XI – MAINTENANCE AND EXCESS EQUIPMENT

38. If any component (i.e. the FORTEZZA® card, the FORTEZZA®-enabled Modem card, or the computer that implements RASP) of the RASP Secret Dial-In Solution should fail, or if the user is disabled/locked-out of the FORTEZZA® card or the FORTEZZA®-enabled Modem card, the user must notify his or her SA and ISSO no later than one working day after discovery for review and further guidance.

39. If the computer that implements RASP requires repair, the user's FORTEZZA® card, the FORTEZZA®-enabled Modem card, and the hard drive must be removed and secured prior to the computer undergoing any maintenance. Maintenance on the computer that implements RASP may only be performed at a Designated Approving Authority (DAA) approved maintenance facility or by a DAA approved maintenance technician.

40. If the RASP solution or its components become excess to a user's needs, the SA should be informed.

ANNEX A

REFERENCES

a. **NAG No. 69C**, Information Systems Security Policy and Procedures for FORTEZZA® Card Certification Authority Workstation, dated Feb 2000.

b. **NSTISSI No. 3028**, Interim Operational Security Doctrine for the FORTEZZA® User PCMCIA Card, dated 10 June 1998.

c. **CSC-STD-002-85**, Department of Defense Password Management Guideline, dated 12 April 1985.

ANNEX B

ACRONYMNS

a. ACL – Access Control List
b. CKL – Compromised Key List
c. COMSEC – Communications Security
d. CRL – Certificate Revocation List
e. DAA – Designated Approving Authority
f. ICRL – Indirect Certificate Revocation List
g. IMO – Intelink Management Office
h. ISSO – Information System Security Officer
i. NSTISSC – National Security Telecommunications Systems Security Committee
j. ORA – Organizational Registration Authority
k. PIN – Personal Identification Number
l. PSTN – Public Switched Telephone Network
m. RASP – Remote Access Security Program
n. SA – System Administrator
o. U.S. – United States
p. VPN – Virtual Private Network